

539.506

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro



17 JUN 2005



(43) Internationales Veröffentlichungsdatum
8. Juli 2004 (08.07.2004)

PCT

(10) Internationale Veröffentlichungsnummer
WO 2004/057824 A1

(51) Internationale Patentklassifikation⁷: H04L 29/06,
H04M 15/00, G06F 17/60

(21) Internationales Aktenzeichen: PCT/EP2003/014632

(22) Internationales Anmeldedatum:
19. Dezember 2003 (19.12.2003)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
102 59 755.3 19. Dezember 2002 (19.12.2002) DE

(71) Anmelder (für alle Bestimmungsstaaten mit Ausnahme von
US): BT (GERMANY) GMBH & CO. OHG [DE/DE];
Elsenheimerstrasse 11, 80687 München (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder (nur für US): ERNST, Matthias
[DE/DE]; Paul-von-Groth-Weg 7, 80999 München (DE).
STÖTTER, Tobias [DE/DE]; Landsbergerstrasse 75,
80339 München (DE). ELBS, Stefan [DE/DE]; Kinbach
9, 88138 Sigmarszell (DE).

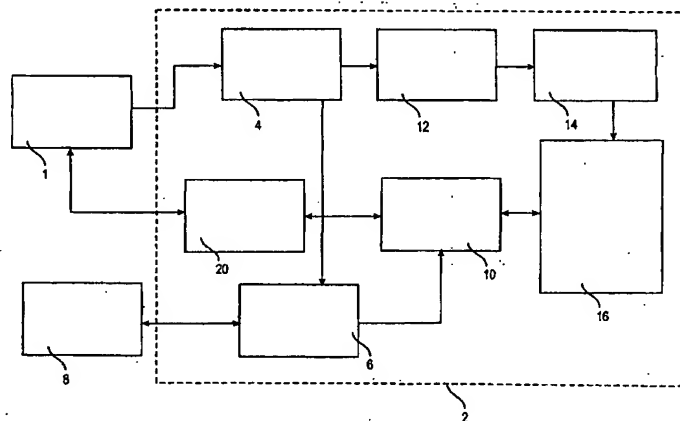
(74) Anwalt: KLANG, Alexander, H.; Wagner & Geyer,
Gewürzmühlstrasse 5, 80538 München (DE).

(81) Bestimmungsstaaten (national): AE, AG, AL, AM, AT,
AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN,
CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI,
GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE,
KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD,
MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH,

[Fortsetzung auf der nächsten Seite]

(54) Title: AUTOMATIC, CONNECTION-BASED TERMINAL OR USER AUTHENTICATION IN COMMUNICATION NETWORKS

(54) Bezeichnung: AUTOMATISCHE ANSCHLUSSBEZOGENE TERMINAL- ODER NUTZERAUTHENTIFIZIERUNG IN KOMMUNIKATIONSNETZEN



(57) Abstract: The aim of the invention is to permit the automatic identification of access rights to protected areas in networks, in particular on the Internet. This is achieved by a method for automatically identifying access rights to protected areas in a first network (2) using a unique connection identifier of a second network (1), in particular in the interconnection of networks that constitutes the Internet. According to the invention: a unique identifier of the first network (2) is dynamically or statically assigned to a terminal, during or prior to the latter's connection to the first network (2); a combination of at least the unique connection identifier of the second network (1) and the unique identifier of the first network (2), said combination being stored in an authentication unit (16), is polled when the terminal requests access to the protected area, in order to determine the unique connection identifier of the second network (1) using the unique identifier of the first network (2); and the existence of access rights to the protected area for the unique connection identifier of the second network (1) is then verified.

(57) Zusammenfassung: Um eine automatische Identifizierung von Zugriffsrechten auf geschützte Bereiche in Netzwerken, insbesondere im Internet zu ermöglichen, sieht die vorliegende Erfindung ein Verfahren zum automatischen Erkennen eines Zugriffsrechts auf geschützte Bereiche in einem ersten Netz (2) unter Verwendung einer eindeutigen Anschlusskennung eines zweiten Netzes (1),

[Fortsetzung auf der nächsten Seite]

WO 2004/057824 A1



PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) **Bestimmungsstaaten (regional):** ARIPO-Patent (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI-Patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Veröffentlicht:

- mit internationalem Recherchenbericht
- vor Ablauf der für Änderungen der Ansprüche geltenden Frist; Veröffentlichung wird wiederholt, falls Änderungen eintreffen

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

insbesondere im Netzwerk des Internets, vor, bei dem eine dynamische oder statische Zuordnung einer eindeutigen Kennung des ersten Netzes (2) für einen Terminal, bei bzw. vor seinem Verbindungsaufbau mit dem ersten Netz (2) erfolgt, eine Kombination aus wenigstens der eindeutigen Anschlusskennung des zweiten Netzes (1) und der eindeutigen Kennung des ersten Netzes (2) in einer Authentifizierungseinheit (16) zum Ermitteln der eindeutigen Anschlusskennung des zweiten Netzes (1) anhand der eindeutigen Kennung des ersten Netzes (2) abgefragt wird, wenn der Terminal auf den geschützten Bereich zugreifen möchte, und geprüft wird, ob für die eindeutige Anschlusskennung des zweiten Netzes (1) ein Zugriffsrecht für den geschützten Bereich besteht.

AUTOMATISCHE ANSCHLUSSBEZOGENE TERMINAL-ODER NUTZERAUTHENTIFIZIERUNG IN KOMMUNIKATIONSNETZEN

Die vorliegende Erfindung bezieht sich auf eine automatische Terminal- oder Nutzeridentifizierung in Netzwerken, insbesondere im Netzverbund des Internets, und insbesondere auf ein Verfahren zum automatischen Erkennen eines Zugriffsrechts auf geschützte Bereiche in Netzwerken, insbesondere im Netzverbund des Internet, wobei der Begriff geschützter Bereich jegliche nicht frei verfügbaren Transaktionen umfasst.

Die Handhabung von sensiblen Daten oder Transaktionen unter Ausschluß Unberechtigter in Netzwerken, insbesondere im frei zugänglichen Internet stellt große Sicherheitsprobleme dar. Einerseits müssen zunächst Zugriffsrechte für die Transaktionen unter Ausschluß Unberechtigter sichergestellt werden und andererseits muss anschließend eine sichere Übertragung der Daten erfolgen. Die vorliegende Erfindung befasst sich mit dem ersten dieser Probleme, nämlich der Prüfung, ob ein Terminal, der Transaktionen unter Ausschluß Unberechtigter durchführt, auch Zugriffsrechte hierfür besitzt.

Ein übliches Verfahren zur Identifizierung eines Terminals oder Nutzers für die Lieferung einer bestimmten Leistung, wie zum Beispiel den Zugriff auf geschützte Bereiche im Internet, ist die Abfrage eines Benutzernamens und eines Passwortes. Ein solches Verfahren, bei dem ein Benutzername und Passwort abgefragt wird, sieht eine relativ hohe Sicherheit hinsichtlich der Identifizierung des Nutzers vor. Bei diesem Verfahren ist es jedoch notwendig, dass sich der Nutzer zunächst in irgendeiner Form registrieren lassen muss, um einen gewünschten Bereich zu nutzen. Dies hat für den Nutzer zur Folge, dass er ggf. persönliche Daten für die Registrierung bereitstellen muss, ohne dass ihm dies Recht wäre. Darüber hinaus schreiben sich Nutzer heutzutage häufig Benutzernamen und Passwörter nieder, da sie zu viele Passwörter oder Pins, z.B. für den Zugriff auf den eigenen Rechner, die Kontokarte, die Kreditkarte etc. verwalten müssen. Das Niederschreiben birgt jedoch bekanntermaßen ein Sicherheitsrisiko. Für den entsprechenden Anbieter des Dienst-

tes bedeutet dies ferner, dass eine entsprechend leistungsfähige Kundendatenverwaltung vorgesehen ist, die in der Regel manueller Pflege bedarf.

Für den Anbieter einer bestimmten Leistung ist es aber oft nicht notwendig, dass der Empfänger der Leistung sich bei ihm in irgendeiner Form registriert. So ist z.B. der Kunde beim offenen Call-by-Call oder beim offenen Internet-by-Call für den Netzbetreiber (Anbieter) anonym. Dem Netzbetreiber, sind lediglich die Anruf-Rufnummer, d.h. eine eindeutige Anschlußkennung eines ansonsten anonymen Kunden, die Zielrufnummer und die Dauer des Anrufs bekannt. Zur Abrechnung werden diese Daten in der Regel zum Inkasso an die Telefongesellschaft des Kunden, beispielsweise die Deutsche Telekom AG, übermittelt. Dabei kann der Kunde für den Anbieter einer bestimmten Leistung völlig anonym bleiben, da außer der eindeutigen Anschlußkennung keine weiteren Informationen über den Kunden erforderlich sind.

Möchte der Netzbetreiber oder Dienstanbieter dem jeweiligen Kunden jedoch Transaktionen unter Ausschluß unberechtigter Dritter anbieten, beispielsweise vertrauliche Daten - wie einen Einzelverbindungs nachweis - zur Verfügung stellen oder den Zugriff auf andere geschützte Bereiche ermöglichen, so war dies bisher nur mit einer vorherigen Registrierung möglich, um sicherzustellen, dass nur autorisierte Terminals auf die jeweiligen Daten zugreifen können.

Der vorliegenden Erfindung liegt daher die Aufgabe zugrunde, eine automatische Identifizierung von Zugriffsrechten auf geschützte Bereiche in Netzwerken, insbesondere im Internet zu ermöglichen.

Erfindungsgemäß wird diese Aufgabe bei einem Verfahren zum automatischen Erkennen eines Zugriffsrechts auf geschützte Bereiche in einem ersten Netz unter Verwendung einer eindeutigen Anschlusskennung eines zweiten Netzes, insbesondere im Netzverbund des Internets, mit folgenden Verfahrensschritten: dynamische oder statische Zuordnung einer eindeutigen Kennung des ersten Netzes für einen Terminal, bei bzw. vor seinem Verbin-

- dungsaufbau mit dem ersten Netz, Speichern einer Kombination aus wenigstens der eindeutigen Anschlußkennung des zweiten Netzes und der eindeutigen Kennung des ersten Netzes in einer Authentifizierungseinheit Abfragen der Authentifizierungseinheit zum Ermitteln der eindeutigen Anschlußkennung des zweiten Netzes anhand der eindeutigen Kennung des ersten Netzes, wenn der Terminal auf den geschützten Bereich zugreifen möchte, Prüfen, ob für die eindeutige Anschlußkennung des zweiten Netzes ein Zugriffsrecht für den geschützten Bereich besteht. Das vorliegende Verfahren ermöglicht somit eine sichere automatische, Erkennung von Zugriffsrechten auf geschützte Bereiche in Netzwerken anhand der Kennungen aus zwei unterschiedlichen Netzen. Eine Vorabregistrierung mittels Benutzername und Passwort sowie der Angabe persönlicher Informationen ist nicht notwendig. Aber selbst bei dem Zugriff auf Bereiche die zusätzlich eine Registrierung erfordern, wie zum Beispiel kostenpflichtige Datenbanken, ermöglicht das erfindungsgemäße Verfahren, dass der Zugriff nur von bestimmten Netzelementen insbesondere bestimmten Telefonanschlüssen (sowohl Mobil- als auch Festnetz) aus möglich ist, was einen Missbrauch selbst bei Verlust oder bewusster Weitergabe von Benutzernamen und Passwort ausschließt.
- 20 Gemäß einer bevorzugten Ausführungsform der Erfindung enthält die in der aktuellen Authentifizierungseinheit gespeicherte Kombination zusätzliche Daten, wie beispielsweise die Einwahl-Rufnummer in das Netzwerk, einen Benutzernamen (Login) und/oder ein Passwort. Diese Daten können eine noch bessere Identifizierung des Terminals ermöglichen, wobei insbesondere der Benutzername und das Passwort automatisch bei der Einwahl in das Netzwerk erzeugt werden können.

- Bei einer besonders bevorzugten Ausführungsform der Erfindung wird die Authentifizierungseinheit nur temporär geführt, so dass es sich im Wesentlichen um eine dynamische Einheit handelt. Vorzugsweise wird die Kombination an Daten aus der Authentifizierungseinheit gelöscht, sobald der Terminal seine Verbindung beendet. Somit wird sichergestellt, dass ein Zugriff auf den ge-

geschützten Bereich nur solange möglich ist, wie eine Verbindung von der eindeutigen Anschlußkennung zu dem Netzwerk besteht.

Bei einem Ausführungsbeispiel der Erfindung ist die eindeutige Kennung des zweiten Netzes eine Anrufrufnummer. Vorzugsweise umfaßt der geschützte Bereich das Bereitstellen eines Online-Einzelverbindungs nachweises, so dass der Nutzer von Call-by-Call oder Internet-by-Call Diensten auf seine Verbindungsnachweise zugreifen kann, ohne sich vorher registrieren zu müssen. Dabei erfolgt der Einzelverbindungs nachweis automatisch für die eindeutige Anschlußkennung des Terminals. Bei einer alternativen Ausführungsform der Erfindung ist vor Freigabe eines Einzelverbindungs nachweises eine weitere Eingabe am Terminal des Nutzers notwendig, um sicherzustellen, dass nicht jeder Terminal, der Zugriff auf ein Bestimmtes Netzelement bzw. einen bestimmten Telefonanschluss besitzt, auch die Verbindungsnachweise dieses Anschlusses abrufen kann. Beispielsweise umfaßt die weitere Eingabe das Eingeben einer Rechnungs- und/oder Kundennummer der Telefongesellschaft, und oder einer PIN.

Um eine hohe Sicherheit bei der Identifizierung sicherzustellen, und einen Missbrauch der Authentifizierungseinheit sicherzustellen haben nur autorisierte Dienste Zugriff auf die Authentifizierungseinheit, die sich ggf. bei der Authentifizierungseinheit vorab registrieren müssen und sich bei der Abfrage identifizieren.

Bei einer Ausführungsform der Erfindung umfaßt der geschützte Bereich wenigstens einen der folgenden Dienste: Bereitstellung von Daten (kostenpflichtige Datenbanken), elektronischer Handel (E-Commerce) und Payment. Im E-Commerce Bereich kann zwar in der Regel eine Vorabregistrierung eines Kunden nicht entfallen, aber die Nutzung der E-Commerce-Dienste kann erleichtert werden, da ein Terminal automatisch anhand seiner Anschlusskennung wie z.B. seinem Telefonanschluss, erkannt werden kann. Bei dem Payment Dienst können Geldbeträge beispielsweise über die Telefonrechnung eines Kunden abgerechnet werden, z.B. die einmalige Abrechnung eines klei-

nen Betrages für das Lesen eines bestimmten Zeitungsartikels im Internet. Die beim Payment Dienst entstehenden Kosten werden vorzugsweise automatisch über die eindeutige Anschlußkennung abgerechnet. Dabei ermöglicht das erfindungsgemäße Verfahren einen nachträglichen exakten Nachweis über den Verbindungsaufbau zwischen zwei Netzelementen, den Kontakt, die
5 Bestellung und ggf. die Lieferung der erbrachten Leistung auch ohne Registrierung des jeweiligen Kunden.

Bei einer weiteren Ausführungsform der Erfindung werden im geschützten Bereich anhand der eindeutigen Anschlußkennung des zweiten Netzes, wie z.B. der Anschlussrufnummer oder SIM Karten Adresse, automatisch weitere Daten des Terminals aufgerufen und/oder weitere Verfahrensschritte eingeleitet. Die zusätzlichen Daten können sich beispielsweise aus einer Vorabregistrierung unter der eindeutigen Anschlußkennung ergeben. Solche zusätzlichen
10 Daten sind insbesondere im E-Commerce Bereich zweckmäßig, wo ggf. Zustell- und Rechnungsadressen eingegeben werden müssen. Als weitere Verfahrensschritte kann z. B. eine automatische Verarbeitung einer Bestellung erfolgen. Das erfindungsgemäße Verfahren kann ferner auch in Kombination mit der bekannten Authentifizierung mit Benutzernamen und Passwort
15 verwendet werden, um eine noch höhere Datensicherheit zu erreichen.
20

Die der Erfindung zugrundeliegende Aufgabe wird auch bei einem Verfahren zum Bereitstellen von Daten für eine automatische Erkennung von Zugriffsrechten auf geschützte Bereiche in Netzen, insbesondere im Netzverbund des Internets, mit folgenden Verfahrensschritten gelöst: Vorsehen von wenigstens
25 jeweils einer eindeutigen Kennung aus wenigstens zwei unterschiedlichen Netzen während eine Verbindung zu beiden Netzen besteht, Speichern einer Kombination der unterschiedlichen Kennungen in einer dynamischen Authentifizierungseinheit, Ausgeben und/oder Authentifizieren einer der eindeutigen
30 Kennungen, bei einer entsprechenden Anfrage hinsichtlich der anderen eindeutigen Kennungen, Löschen der Daten aus der dynamischen Authentifizierungseinheit sobald eine Verbindung mit wenigstens einem der beiden Netze beendet wurde. Das erfindungsgemäße Verfahren sieht eine dynamische Au-

thentifizierungseinheit von aktuell im Netzwerk befindlichen Terminals vor, die eine Identifizierung eines Terminals anhand seiner eindeutigen Kennung aus beiden Netzwerken ermöglicht. Dabei wird die Authentifizierungseinheit in Echtzeit geführt, sodass die gespeicherten Daten nur solange vorgehalten
5 werden, wie der Terminal im Netzwerk ist. Nach Beenden der Verbindung werden die Daten umgehend gelöscht, um einen Missbrauch zu verhindern.

Vorzugsweise ist wenigstens eine der Kennungen eine IP-Nummer und/oder
10 eine eindeutigen Anschlußkennung eines Terminals.

Für eine erhöhte Datensicherheit wird geprüft, dass die Anfrage hinsichtlich einer bestimmten IP-Nummer von einem autorisierten Dienst stammt. Hierdurch wird sichergestellt, dass die in der Authentifizierungseinheit befindlichen Daten nicht missbräuchlich verwendet werden.

15 Für eine erhöhte Datensicherheit sind in der aktuellen Authentifizierungseinheit zu der oben genannten Kombination zusätzliche Daten gespeichert. Diese können beispielsweise die Einwahl-Rufnummer, einen Benutzernamen (Login) und ein Passwort umfassen. Diese zusätzlichen Daten sehen eine
20 noch erhöhte Identifizierungssicherheit vor.

Bei einer Ausführungsform der Erfindung kann über die Authentifizierungseinheit bzw.. die ausgegebene Kennung eine Anruf-Rufnummernsperre oder eine Ziel-Rufnummernsperre identifiziert werden.

25 Die vorliegende Erfindung wird nachfolgend anhand eine bevorzugten Ausführungsbeispiels der Erfindung unter Bezugnahme auf die Zeichnung näher erläutert. In der Zeichnung zeigt:

30 Fig. 1 eine schematische Systemübersicht für einen offenen Internet-by-Call Dienst eines Telekommunikations-Netzbetreibers.

Anhand der Fig. 1 wird das erfindungsgemäße Verfahren bei einer automatischen Erkennung von Zugriffsrechten am Beispiel eines Online Einzelverbindungs nachweises (EVN) für Internet-by-Call Kunden näher erläutert.

- 5 Zunächst wird jedoch der allgemeine Abrechnungsmodus bei einem Internet-by-Call Dienst beschrieben. Bei einem offenen Internet-by-Call Dienst wählt sich ein Kunde, dessen Anschluss beispielsweise auf die Deutsche Telekom AG (DTAG) läuft, über das Netz der DTAG in das Netzwerk eines entsprechenden Netzbetreibers, der nachfolgend als Anbieter bezeichnet wird, ein.
- 10 Die DTAG vermittelt den entsprechenden Anruf in ihrem Netz bis zu einem definierten Übergabepunkt, der auch als point of interconnect (POI) bezeichnet wird. An diesem POI wird der Anruf von der DTAG an den Anbieter des Internet-by-Call Dienstes übergeben. Gegebenenfalls kommt es nun zu einer Vermittlung des Anrufs im Netz des Anbieters, und der Anruf wird auf einer
- 15 Modembank des Anbieters terminiert. Sofern erforderlich, werden die Kundendaten, wie beispielsweise ein Benutzername und ein Passwort geprüft und anschließend wird dem Kunde eine (dynamische) IP-Adresse zugewiesen. Nun wird der Anruf auf Basis des Internet-Protokolls (IP) bis zu seiner Zieldestination (z.B. dem öffentlichen Internet) weitervermittelt.
- 20 Die zur Abrechnung des Anrufs relevanten Daten werden von dem Anbieter festgehalten, und zum Inkasso an die DTAG weitergeleitet.
- Der Anbieter bekommt von der DTAG Informationen hierüber, welche Datensätze auf welcher Rechnungsnummer (Rechnungsnummer, Kundennummer
- 25 sowie Rechnungsdatum) abgerechnet wurden, ohne dass dem Anbieter die Personalien des Kunden bekannt sind.
- Die DTAG listet auf ihren Rechnungen nicht die einzelnen Internet-by-Call Anrufe des Kunden auf, die dieser aber, wie nachfolgend beschrieben wird, Online abfragen kann.
- 30

Das nachfolgend unter Bezugnahme auf Fig. 1 beschriebene System ermöglicht eine automatische anschlussbezogene Authentifizierung eines Kunden, um den Zugriff auf einen Online-Einzelverbindungs-nachweis eines Internet-by-Call Anbieters zu ermöglichen.

5

Block 1 in Fig. 1 stellt das Telekommunikationsnetz außerhalb des Netzwerks des Anbieters dar. Im Block 1 erfolgt somit die Einwahl und die Vermittlung des Anrufs bis zum POI des Internet-by-Call Anbieters.

- 10 Das System des Netzanbieters ist durch einen gestrichelten Kasten 2 in Fig. 1 dargestellt.

Der Block 4 in Fig. 1 repräsentiert einen Switch, in dem die zur Abrechnung des Kunden relevanten Daten erzeugt werden. Diese Kundendaten, die als
15 Call-Data-Records (CDR) bezeichnet werden, enthalten z.B. die eindeutige Anschlußkennung des Kunden, die Einwahl-Rufnummer in das Netzwerk des Anbieters und die Start- sowie die Endzeit des Anrufs. Diese Daten werden im Netz des Anbieters zu einem Berechnungssystem im Block 6 weitergeleitet, das die Kosten für den jeweiligen Anruf berechnet. Die berechneten Kosten
20 werden unter Angabe der eindeutigen Anschlußkennung an die DTAG im Block 8 übermittelt. Die DTAG stellt diese Kosten nachfolgend dem Kunden des jeweiligen Anschlusses der eindeutigen Anschlußkennung in Rechnung und liefert Daten betreffend die Rechnungsstellung zurück an das Berechnungssystem im Block 6. Diese Daten enthalten beispielsweise die Rechnungsnummer, die Kundennummer sowie das Rechnungsdatum. Nicht enthal-
25 ten sind die persönlichen Daten des Kunden.

Vom Block 6 werden die berechneten Kosten gemeinsam mit den CDR-Daten zu einem netzinternen Datenbankserver im Block 10 übermittelt. Diese Über-
30 mittlung kann sofort oder erst nach Erhalt der Rechnungsdaten durch die DTAG erfolgen. Wenn die Übermittlung der Daten sofort erfolgt, werden die später von der DTAG zurückgesandten Rechnungsdaten nach Erhalt nach-

träglich an den Datenbankserver 10 übermittelt, welche diese Daten dann kumuliert bzw. gesteuert.

Der Switch im Block 4 leitet einen Teil der CDR-Daten, nämlich die eindeutige
5 Anschlußkennung und die Einwahl-Rufnummer an eine Modembank im Block
12 weiter, wo der Anruf terminiert wird. Von der Modembank im Block 12 wer-
den die Daten an einen Server im Block 14 übermittelt. Dort wird eine aktuelle
IP-Adresse für den Anruf verteilt. Die aktuelle IP-Adresse, sowie die dazuge-
hörige eindeutige Anschlußkennung und die Einwahl-Rufnummer werden an-
10 schließend an eine Authentifizierungseinheit im Block 16 weitergeleitet. Wenn
der Anruf beendet ist, d.h. die Verbindung zwischen dem Netzwerk des Anbie-
ters und dem Kunden getrennt wird, teilt der Switch im Block 4 der Modem-
bank im Block 12 mit, dass der Anruf beendet wird. Der entsprechende Platz
an der Modembank wird freigegeben, und die Modembank teilt dem Server im
15 Block 14 unter Angabe der entsprechenden IP-Adresse mit, dass der Anruf
beendet wurde. Der Server im Block 14 wiederum überträgt diese Information
sofort an die Authentifizierungseinheit, in der die Daten aus IP-Adresse, ein-
deutiger Anschlußkennung und Einwahl-Rufnummer sofort gelöscht werden.
Die Authentifizierungseinheit beinhaltet somit eine dynamische Datenbank, in
20 der jeweils nur aktuelle Authentifizierungsdaten gespeichert sind, d.h. Daten
betreffend eine aktuelle Verbindung zwischen einem Anschluss eines Kunden
(eindeutigen Anschlußkennung) und einem Einwahlpunkt des Netzwerkes
(Einwahl-Rufnummer) sowie die dynamisch zugewiesene IP-Adresse. Diese
bestimmte Kombination an Daten wird nur solange gespeichert, wie eine tat-
25 sächliche Verbindung zu einem Anschluss des Kunden besteht.

Möchte ein Kunde nun seine Rechnungsdaten Online einsehen, so wird er im
Netzwerk des Anbieters die entsprechende Internetseite, die Zugriff auf den
Datenbankserver im Block 10 besitzt, über ein Webinterface im Block 20 auf-
30 rufen. Über das Webinterface wird der Datenbankserver 10 zwar die aktuell
zugewiesene IP-Nummer des Kunden mitgeteilt, nicht jedoch dessen eindeu-
tigen Anschlußkennung. Der Datenbankserver im Block 10 stellt daher eine
Anfrage an die Authentifizierungseinheit im Block 16, um festzustellen, ob die

bei der Anfrage verwendete IP-Adresse des Kunden eine aktuelle IP-Adresse darstellt, und ferner, welchem Anschluss, d.h. welcher eindeutigen Anschlußkennung, die IP-Adresse zugewiesen wurde. Wenn es sich um eine aktuelle IP-Adresse handelt, wird die Datenkombination aus der Authentifizierungseinheit an den Datenbankserver im Block 10 geliefert, und der Datenbankserver kann nun die der eindeutigen Anschlußkennung zugehörigen Einzelverbindungs-nachweise herausfiltern und zur Einsicht freigeben. Gegebenenfalls können auch zusätzliche Informationen, wie beispielsweise eine PIN und/oder eine Rechnungs- und/oder Kundennummer der DTAG angefordert werden, um die Information hinsichtlich des Einzelverbindungs-nachweises auch nur der Person bzw. dem Terminal zur Verfügung zustellen, die bzw. der tatsächlich Zugriff auf die Rechnung der DTAG besitzt.

Das wesentliche Merkmal für eine sichere, anschlussbezogene Identifizierung eines Terminals ist das Vorsehen der dynamischen Authentifizierungseinheit, die nur Daten für aktuell bestehende Verbindungen enthält, und somit eine hohe Sicherheit gegen Missbrauch bietet.

Obwohl die vorliegende Erfindung speziell anhand eines Online Einzelverbindungs-nachweises beschrieben wurde, ist die anschlussbezogene Authentifizierung von Zugriffsrechten natürlich auch auf andere Gebiete ausweitbar. Beispielsweise könnte ein beliebiger netzinterner oder auch netzexterner Dienst auf die Authentifizierungseinheit zugreifen, um festzustellen, ob und welchem Telefonanschluss (eindeutige Anschlußkennung) eine bestimmte IP-Adresse aktuell zugewiesen ist. Die eindeutige Anschlußkennung läßt nunmehr eine anschlussbezogene Authentifizierung durch den jeweiligen Dienst zu. Dabei dürfen natürlich nur bestimmte registrierte Dienste auf die Authentifizierungseinheit zugreifen, die sich auch jeweils gesondert identifizieren müssen, um einen Missbrauch der Authentifizierungseinheit zu verhindern.

30

Solche Dienste sind beispielsweise Payment Dienste, welche Beträge über ein entsprechendes Inkassosystem über die Telefonrechnung der DTAG abrechnen. Eine derartige Abrechnung erfolgt beispielsweise beim kostenpflich-

tigen Lesen bestimmter Zeitungsartikel im Internet. Ein Nachweis über das Zustandekommen der Verbindung, die Bestellung, die Lieferung und somit für die Durchsetzung von Zahlungsansprüchen bzw. Lieferverpflichtungen ist somit über das obige Authentifizierungsverfahren auch bei "anonymen" Endkunden möglich.

Eine weitere Möglichkeit der Nutzung einer anschlussbezogenen Authentifizierung ist die Identifizierung durch E-Commerce Anbieter. Bei Bestellungen oder Anfragen an E-Commerce Anbieter können diese automatisch eine anschlussbezogene Authentifizierung vornehmen und somit Bestellungen eindeutig zuordnen. Dies ist insbesondere beim Kauf virtueller Produkte (z.B. Digitale Bücher, Ton- und Filmaufnahmen) Vorteilhaft, da hier die Lieferadresse keine Kontrolle darstellt. Eine weitere Authentifizierung über Benutzername und Kennwort kann dann entfallen oder zusätzlich eingesetzt werden, um eine noch höhere Sicherheit zu bieten. Anhand der anschlussbezogenen Authentifizierung kann der E-Commerce Anbieter weitere relevante Daten des Kunden aufrufen, sofern der Kunde mit der eindeutigen Anschlußkennung registriert ist.

E-Commerce Anbieter und auch Anbieter anderer Inhalte können verschiedene eindeutige Anschlußkennungen beim Netzbetreiber sperren lassen, um zu verhindern, dass weitere Transaktionen von diesen Anschlüssen aus vorgenommen werden. Insofern sieht die anschlussbezogene Authentifizierung einen Schutz gegen Missbrauch vor.

Ein weiteres Beispiel, bei dem die anschlussbezogene Authentifizierung von besonderem Nutzen sein kann, ist die Registrierung bei bestimmten Diensten über die eindeutige Anschlußkennung. Der Kunde kann beispielsweise seinen Anschluss für bestimmte Dienste freischalten lassen, und erhält daraufhin einen automatisch erzeugten Code, den er in Zukunft im Nachwahlverfahren an die Einwahl-Rufnummer anhängt. Mittels dieses Codes kann der entsprechenden eindeutigen Anschlußkennung ein bestimmter Satz an Diensten zu-

geordnet werden, die für diese eindeutige Anschlußkennung genehmigt sind (z.B. nur online-tarifizierte Dienste, keine XXX-Dienste).

Auch bei einem Online-Behördengang kann der Nutzer bzw. ein Terminal sicher identifiziert werden, um Missbrauch zu vermeiden. Die anschlussbezo-
5 gene Identifizierung kann in vielen Fällen eine elektronische Signatur ersetzen und ermöglicht ferner die Übertragung von aus den Telefonnetzen bekannten Zahlungsmodellen auf die Datennetze.

- 10 Die anschlussbezogene Identifizierung ermöglicht allgemein das zur Verfügung stellen von Inhalten unter Ausschluß Dritter ohne eine weitere Authentifizierung sowie das Sperren von Inhalten für eine eindeutige Anschlußkennung. Anhand der anschlusstechnischen Information lässt sich ferner überprüfen, ob eine bestimmte Leistung für diesen Anschluss sinnvoll ist. So macht
15 es keinen Sinn, einen Videostream auf ein GSM-Handy zu übertragen, während dies für ein UMTS Endgerät oder einen Festnetzanschluss mit Terminal durchaus sinnvoll sein kann.

- Die vorliegende Erfindung ist nicht auf das konkret ausgeführte Ausführungs-
20 beispiel und die oben genannten Beispiele beschränkt. Vielmehr sieht sie allgemein eine automatische Authentifizierung eines Terminals in Netzwerken, insbesondere im Netzverbund des Internets vor, bei der wenigstens zwei Kennungen aus wenigstens zwei unterschiedlichen Netzen eingesetzt werden. Die Authentifizierung kann für verschiedene Zwecke eingesetzt werden.

Patentansprüche

- 1 Verfahren zum automatischen Erkennen eines Zugriffsrechts auf ge-
schützte Bereiche in einem ersten Netz unter Verwendung einer ein-
5 deutigen Anschlusskennung eines zweiten Netzes, insbesondere im
Netzverbund des Internets, mit folgenden Verfahrensschritten:
- dynamische oder statische Zuordnung einer eindeutigen Kennung
des ersten Netzes für einen Terminal, bei bzw. vor seinem Verbin-
dungsaufbau mit dem ersten Netz;
 - 10 - Speichern einer Kombination aus wenigstens der eindeutigen
Anschlußkennung des zweiten Netzes und der eindeutigen Ken-
nung des ersten Netzes in einer Authentifizierungseinheit;
 - Abfragen der Authentifizierungseinheit zum Ermitteln der eindeuti-
gen Anschlußkennung des zweiten Netzes anhand der eindeutigen
15 Kennung des ersten Netzes, wenn der Terminal auf den geschütz-
ten Bereich zugreifen möchte;
 - Prüfen, ob für die eindeutige Anschlußkennung des zweiten Netzes
ein Zugriffsrecht für den geschützten Bereich besteht.
- 20 2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass die in der
aktuellen Authentifizierungseinheit gespeicherte Kombination zusätzlich
weitere Daten enthält.
3. Verfahren nach Anspruch 2, dadurch gekennzeichnet, dass die zusätz-
25 lichen Daten wenigstens eines der folgenden aufweisen: die Einwahl-
Rufnummer in das erste Netzwerk, einen Benutzernamen (Login) und
ein Passwort.
4. Verfahren nach einem der vorhergehenden Ansprüche, dadurch ge-
30 kennzeichnet, dass die Authentifizierungseinheit nur temporär geführt
wird.

5. Verfahren nach Anspruch 4, dadurch gekennzeichnet, dass die Kombination an Daten aus der Authentifizierungseinheit gelöscht wird, sobald der Terminal seine Verbindung mit einem der beiden Netze beendet.
- 5 6. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die eindeutige Kennung des zweiten Netzes eine Anrufnummer ist.
- 10 7. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass der geschützte Bereich das Bereitstellen eines Online Einzelverbindungs nachweises umfaßt.
- 15 8. Verfahren nach Anspruch 7, dadurch gekennzeichnet, dass ein Einzelverbindungs nachweis automatisch für die eindeutige Anschlußkennung des zweiten Netzes erfolgt.
- 20 9. Verfahren nach Anspruch 7, dadurch gekennzeichnet, dass vor Freigabe eines Einzelverbindungs nachweises zusätzliche eine weitere Eingabe am Terminal notwendig ist.
- 10 10. Verfahren nach Anspruch 9, dadurch gekennzeichnet, dass die weitere Eingabe das Eingeben einer Rechnungsnummer und/oder einer Kundennummer und/oder einer PIN umfaßt.
- 25 11. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass nur autorisierte Dienste Zugriff auf die Authentifizierungseinheit haben.
- 30 12. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass der geschützte Bereich wenigstens einen der folgenden Dienste beinhaltet: Bereitstellen von Inhalten, elektronischer Handel (E-commerce), Payment bzw. Zahlungsdienste und Behörden-dienste.

13. Verfahren nach Anspruch 12, dadurch gekennzeichnet, dass bei einem Payment Dienst die entstehenden Kosten automatisch über die eindeutige Anschlußkennung des zweiten Netzes abgerechnet werden.

5

14. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass im geschützten Bereich anhand der eindeutigen Anschlußkennung des zweiten Netzes automatisch weitere Daten des Terminals aufgerufen werden und/oder weitere Verfahrensschritte eingeleitet werden.

10

15. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass eine weitere Personalisierung des Terminals über die Eingabe einer PIN erfolgt.

15

16. Verfahren zum Bereitstellen von Daten für eine automatische Erkennung von Zugriffsrechten auf geschützte Bereiche in Netzen, insbesondere im Netzverbund des Internets, mit folgenden Verfahrensschritten:
- Vorsehen von wenigstens jeweils einer eindeutigen Kennung aus wenigstens zwei unterschiedlichen Netzen während eine Verbindung zu beiden Netzen besteht;
 - Speichern einer Kombination der unterschiedlichen Kennungen in einer Authentifizierungseinheit;
 - Ausgeben und/oder Authentifizieren einer der eindeutigen Kennungen, bei einer entsprechenden Anfrage hinsichtlich der anderen eindeutigen Kennungen;
 - Löschen der Daten aus der Authentifizierungseinheit sobald eine Verbindung mit wenigstens einem der beiden Netze beendet wurde.

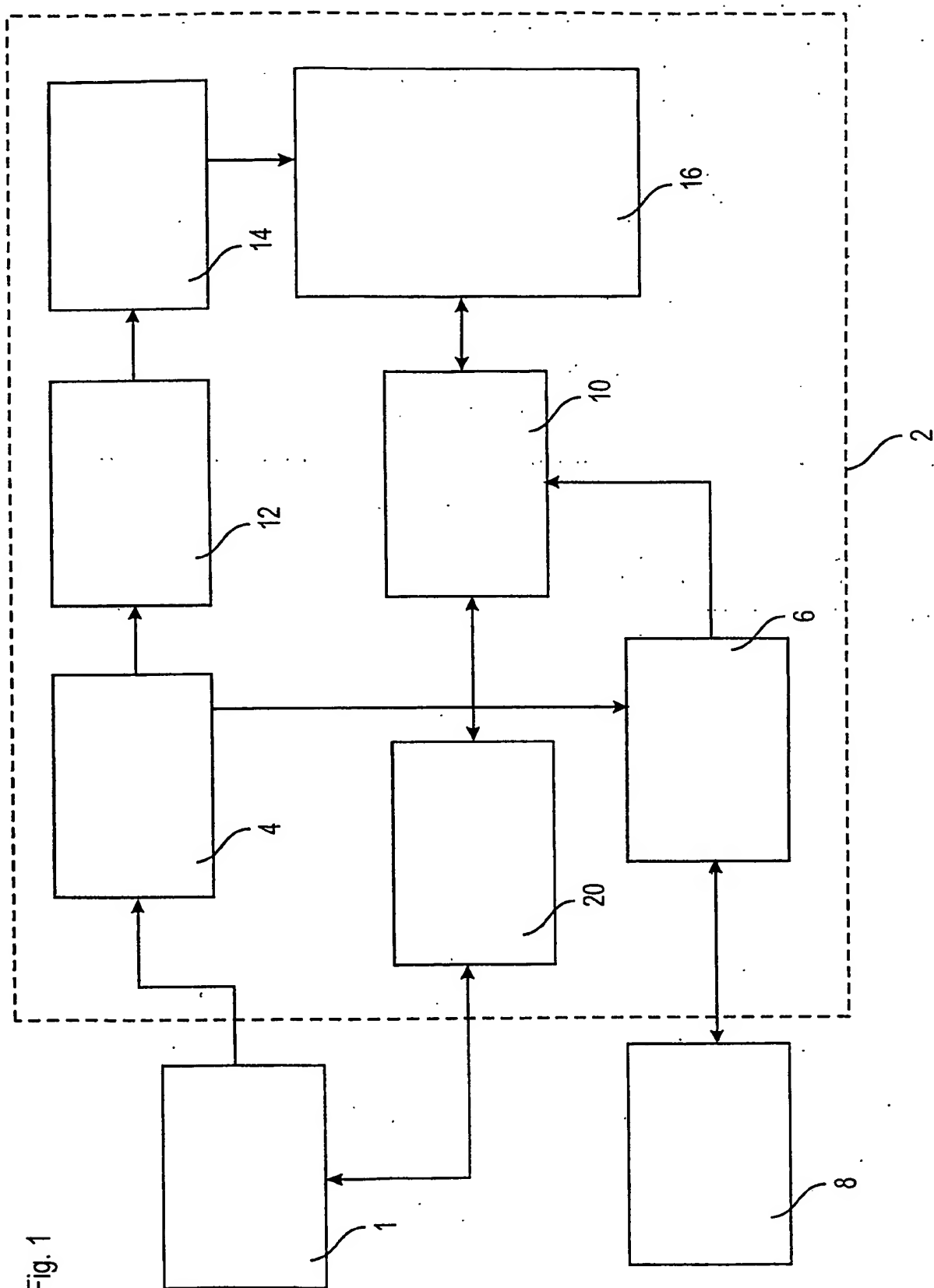
20

25

17. Verfahren nach Anspruch 16, dadurch gekennzeichnet, dass wenigstens eine der Kennungen eine IP-Nummer und/oder eine eindeutige Anschlußkennung eines Terminals ist.

30

18. Verfahren nach Anspruch 16 oder 17, dadurch gekennzeichnet, dass geprüft wird, ob die Anfrage von einer autorisierten Stelle bzw. einem autorisierten Dienst stammt.
- 5 19. Verfahren nach einem der Ansprüche 16 bis 18, dadurch gekennzeichnet, dass die in der aktuellen Authentifizierungseinheit gespeicherte Kombination zusätzlich weitere Daten enthält.
- 10 20. Verfahren nach Anspruch 19, dadurch gekennzeichnet, dass die zusätzlichen Daten wenigstens eines der folgenden aufweisen: eine Einwahl-Rufnummer in eines der Netze, einen Benutzernamen (Login) und ein Passwort.
- 15 21. Verfahren nach einem der Ansprüche 16 bis 20, dadurch gekennzeichnet, dass über die Authentifizierungseinheit eine Anruf-Rufnummernsperre oder eine Ziel-Rufnummernsperre identifiziert wird.



INTERNATIONAL SEARCH REPORT

International Application No.

PCT/EP 03/14632

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06 H04M15/00 G06F17/60

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 H04L H04M G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data, PAJ, INSPEC, COMPENDEX, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 6 400 812 B1 (BERGLUND JAN ET AL) 4 June 2002 (2002-06-04) column 3, line 18 -column 4, last line figures 1-6	1-24
X	PATENT ABSTRACTS OF JAPAN vol. 2002, no. 11, 6 November 2002 (2002-11-06) & JP 2002 207929 A (NIPPON TELEGR & TELEPH CORP), 26 July 2002 (2002-07-26) abstract	1-24
X	US 6 151 628 A (XU YINGCHUN ET AL) 21 November 2000 (2000-11-21) column 5, line 9-43 column 5, line 61 -column 6, line 37 column 11, line 20 -column 13, line 11 column 14, line 65 -column 17, line 22	1-24
	-/-	

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

- "A" document defining the general state of the art which is not considered to be of particular relevance
- "E" earlier document but published on or after the international filing date
- "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- "O" document referring to an oral disclosure, use, exhibition or other means
- "P" document published prior to the international filing date but later than the priority date claimed

- "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- "&" document member of the same patent family

Date of the actual completion of the international search

22 April 2004

Date of mailing of the international search report

28/04/2004

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3018

Authorized officer

Bengi-Akyuerek, K

INTERNATIONAL SEARCH REPORT

International Application No

PCT/EP 03/14632

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
P, X	EP 1 284 575 A (NTT DOCOMO INC) 19 February 2003 (2003-02-19) paragraphs '0032!-'0045! figures 1-3	1-24
X	& WO 02/078307 A (NAKAJIMA TAKAYUKI; NTT DOCOMO INC (JP)) 3 October 2002 (2002-10-03)	1-24
A	PATENT ABSTRACTS OF JAPAN vol. 1999, no. 02, 26 February 1999 (1999-02-26) & JP 10 294759 A (CASIO COMPUT CO LTD), 4 November 1998 (1998-11-04) abstract	1-24

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/EP 03/14632

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
US 6400812	B1	04-06-2002	SE 520137 C2 AU 6426198 A CN 1135782 B EP 0966811 A1 JP 2001517390 T SE 9700870 A WO 9840985 A1	03-06-2003 29-09-1998 21-01-2004 29-12-1999 02-10-2001 12-11-1998 17-09-1998
JP 2002207929	A	26-07-2002	NONE	
US 6151628	A	21-11-2000	AU 8181498 A CA 2264866 A1 DE 69803974 D1 DE 69803974 T2 EP 0927482 A1 IL 128656 A JP 2000503198 T WO 9901969 A1	25-01-1999 14-01-1999 04-04-2002 07-11-2002 07-07-1999 29-05-2003 14-03-2000 14-01-1999
EP 1284575	A	19-02-2003	EP 1284575 A1 CN 1460355 T WO 02078307 A1 US 2003169714 A1	19-02-2003 03-12-2003 03-10-2002 11-09-2003
JP 10294759 9	A		NONE	

INTERNATIONAL RECHERCHENBERICHT

Internationales Aktenzeichen

PCT/EP 03/14632

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 H04L29/06 H04M15/00 G06F17/60

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierte Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)

IPK 7 H04L H04M G06F

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der Internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

EPO-Internal, WPI Data, PAJ, INSPEC, COMPENDEX, IBM-TDB

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	US 6 400 812 B1 (BERGLUND JAN ET AL) 4. Juni 2002 (2002-06-04) Spalte 3, Zeile 18 -Spalte 4, letzte Zeile Abbildungen 1-6	1-24
X	PATENT ABSTRACTS OF JAPAN vol. 2002, no. 11, 6. November 2002 (2002-11-06) & JP 2002 207929 A (NIPPON TELEGR & TELEPH CORP), 26. Juli 2002 (2002-07-26) Zusammenfassung	1-24
X	US 6 151 628 A (XU YINGCHUN ET AL) 21. November 2000 (2000-11-21) Spalte 5, Zeile 9-43 Spalte 5, Zeile 61 -Spalte 6, Zeile 37 Spalte 11, Zeile 20 -Spalte 13, Zeile 11 Spalte 14, Zeile 65 -Spalte 17, Zeile 22	1-24
	-/-	

☒ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen☒ Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :

"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden

"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche

22. April 2004

Absendedatum des internationalen Recherchenberichts

28/04/2004

Name und Postanschrift der internationalen Recherchenbehörde
Europäisches Patentamt, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Bevollmächtigter Bediensteter

Bengi-Akyurek, K

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
P,X	EP 1 284 575 A (NTT DOCOMO INC) 19. Februar 2003 (2003-02-19) Absätze '0032!-'0045! Abbildungen 1-3	1-24
X	& WO 02/078307 A (NAKAJIMA TAKAYUKI; NTT DOCOMO INC (JP)) 3. Oktober 2002 (2002-10-03)	1-24
A	PATENT ABSTRACTS OF JAPAN vol. 1999, no. 02, 26. Februar 1999 (1999-02-26) & JP 10 294759 A (CASIO COMPUT CO LTD), 4. November 1998 (1998-11-04) Zusammenfassung	1-24

INTERNATIONALES RESEARCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Patenzeich

PCT/EP 03/14632

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US 6400812	B1	04-06-2002	SE 520137 C2 03-06-2003
		AU 6426198 A 29-09-1998	
		CN 1135782 B 21-01-2004	
		EP 0966811 A1 29-12-1999	
		JP 2001517390 T 02-10-2001	
		SE 9700870 A 12-11-1998	
		WO 9840985 A1 17-09-1998	
JP 2002207929	A	26-07-2002	KEINE
US 6151628	A	21-11-2000	AU 8181498 A 25-01-1999
		CA 2264866 A1 14-01-1999	
		DE 69803974 D1 04-04-2002	
		DE 69803974 T2 07-11-2002	
		EP 0927482 A1 07-07-1999	
		IL 128656 A 29-05-2003	
		JP 2000503198 T 14-03-2000	
		WO 9901969 A1 14-01-1999	
EP 1284575	A	19-02-2003	EP 1284575 A1 19-02-2003
		CN 1460355 T 03-12-2003	
		WO 02078307 A1 03-10-2002	
		US 2003169714 A1 11-09-2003	
JP 10294759 9	A		KEINE